UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/970,912	10/04/2001	Perry J. Robertson	SD-6769	3158

20567   7590   03/03/2006

SANDIA CORPORATION
P O BOX 5800
MS-0161
ALBUQUERQUE, NM 87185-0161

EXAMINER
SHIFERAW, ELENI A

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 03/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

> A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
> - Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
> - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
> - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>02 December 2005</u>.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-21</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>1-21</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☒ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on 12/02/2005 has been entered.

2.   Applicant's amendments/arguments with respect to claims 1-20 have been considered but

are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4.   Claims 1-21 are rejected under 35 U.S.C. 102(b) as being anticipated by Michelle L.

Hankins, SIGNAL AFCEA'S International Journal, October 1999 "Integrated Circuit Chip

Provides Secure, Rapid Data Encryption".

Regarding claims 1, 7, 12, and 17, Michelle L. Hankins discloses a method/apparatus of

enhancing throughput of multi-stage pipelined encryption/decryption engine for an

encryption/decryption process comprising a predetermined number of stages and providing

feedback around the stages (pages 1-3), the method comprising the steps of:

for each of a plurality of encryption/decryption contexts, a number of which equals or

exceeds the predetermined number of stages, receiving, for input to the multi-stage pipeline

encryption/decryption engine, a source datablock for the corresponding encryption context

identifier (page 2 lines 11-22);

for each of the plurality of encryption/decryption contexts, indexing according to the

encryption/decryption context identifier into a bank of variables comprising initial variables and

the bank comprising plurality of initial variables for each encryption/decryption context

identifier and prior-stage output datablocks to retrieve a seed variable for the source datablock

(page 2 lines 6-22); and

for each of the plurality of encryption/decryption contexts, generating an output

datablock from the source datablock and its corresponding seed variable (page 2 lines 11-14);

wherein each stage of the pipelined encryption/decryption engine at any given time is

processing source datablocks from an encryption/decryption context different than

encryption/decryption contexts of source datablocks being processed in all other stages of the

pipelined encryption/decryption engine (page 2 lines 6-page 3 lines 6).

Regarding claims 2 and 13, Michelle L. Hankins teaches the method/apparatus, wherein in the

indexing step/means the bank of initial variables comprises a number of initial variables for each

encryption/decryption context identifier that is at least as large as the predetermined number of

stages (page 2 lines 6-22).

Regarding claims 3 and 14, Michelle L. Hankins teaches the method/apparatus, additionally

comprising the step/means of replacing the corresponding initial variable with the output

datablock (page 2 lines 11-14).

Regarding claims 4, 10, 15, and 20, Michelle L. Hankins teaches the method/apparatus, wherein

the encryption/decryption process comprises Cipher Block Chaining Mode with exception of

handling of initial variables (page 2 lines 2-4).

Regarding claim 5, Michelle L. Hankins teaches the method, wherein the encryption/decryption

process comprises a block cipher capable of being pipelined (page 2 lines 19-22).

Regarding claims 6 and 16, Michelle L. Hankins teaches the method/apparatus, wherein the

process is Digital Encryption Standard (DES) (page 3 lines 1-5).

Regarding claims 8 and 18, Michelle L. Hankins teaches the method/apparatus, wherein each of

the plurality of encryption/decryption contexts comprises a data stream to be encrypted (page 1

par. 1).

Regarding claims 9 and 19, Michelle L. Hankins teaches the method/apparatus, additionally

comprising the step of decrypting the output datablocks at a plurality of locations distributed

from the encryption/decryption engine corresponding in number to the number of

encryption/decryption contexts (page 2 lines 15-18 and lines 31-32).

Regarding claims 11 and 21, Michelle L. Hankins teaches the method/apparatus, wherein the

encryption/decryption process comprises a block cipher capable of being pipelined such as

Digital Encryption Standard (DES) (pages 2-3). .

Conclusion

5.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure. US 6,870,929 B1 Greene *discloses applying multiple different data blocks contexts to*

an encryption circuit having pipelined cipher stages and feedback-type encryption in using

multiple stored initial vectors/seed data block values (IVA-IVD) of CBC/DES engine.

US 6,920,562 B1 Kerr et al. discloses the well-known multi-stage pipelining and DES

encryption.

For more prior art of record please see Form PTO 892 attached.

6.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867.

The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.

February 24, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100